Enclosure 48 – Memorandum of Understanding (MOU) (Sample)

Note to Template User: This must be appropriately modified for the situation.

MEMORANDUM OF UNDERSTANDING

Between

(Name of User Agency)

and

Defense Security Service

References: (a) NISPOM, Chapter 8
(b) (User Agency Regulation)

This Memorandum of Understanding (MOU) between (User Agency) and the Defense Security Service (DSS), Designated Approval Authority for (Company Name), is for the purpose of establishing a secure communications link between (User Agency) and (Company Name) for the electronic transfer of classified information. Each of the undersigned agrees to and understands the procedures that will be in effect and adhered to. It is also understood that this MOU summarizes the information system (IS) security requirements for approval purposes and supplements (Company Name) approved system security plan (SSP).

1. Contract Information

This MOU describes the classified network arrangement between (Company Name) and (User Agency) in support of the (Name of Program). The (Name of Program) is a (brief description of program) sponsored by (User Agency). The contract number is (Contract Number). The prime contractor is (Name of Prime Contractor), whose Cage Code is (Cage Code Number).

(Optional) The following (Name of Company) key points of contact are identified:

NAME	TITLE	PHONE
	Manager of Security	
	Program Manager	
	Program Security Supervisor	
	Information Systems Security Manager (ISSM)	

At (User Agency) direction, (Company or User Agency Name) is establishing a remote access capability to the (Name of Classified Computer System); with a remote access IS located at (User Agency or Company, as appropriate). (Note to Template User: Please word this paragraph so that it is obvious who will be the host, if applicable, and who will be the remote computer system). This capability will allow (Company or User Agency, as appropriate) personnel to access the (Name of Classified IS) as remote users. The (User Agency) IS is located at (address).

(Optional) The following (User Agency) key points of contact are identified:

NAME	TITLE	PHONE

Technical Point of Contact

Information Systems Security Officer

2. Description

(Company or User Agency Name) operates the (Name of Classified System) IS at Protection Level 1, whereby all users have the clearance and need to know for all information on the system. The highest level of classification of the IS is (Level of Information). All personnel with access to the (Name of Classified System) will be briefed for (Give name of specific briefing, e.g. COMSEC).

(Describe connection. An example follows): The (Company Name) IS will be connected to the (Name of Classified System) at (Company Name), by a 9.6 kilobit per second (kbps) communications circuit for the transfer of data via a public switched telephone network. The circuit will be protected at each end by a STU-III telephone modem access, to provide encryption of the circuit. Operational key for the STU-III shall be at the SECRET level.

3. Network Information System Security Officer (Network ISSO) Responsibilities

The Network ISSO at (host--Company or User Agency Name) will have the following responsibilities. He or she will brief operator personnel involved with use of the communications link on network operating procedures and their responsibilities for safeguarding classified information in accordance with the requirements of paragraph 5-100 of the National Industrial Security Program Operating Manual (NISPOM). The IS Security Officer at (Name of other User Agency or Company Site) will conduct an equivalent briefing for network responsible personnel.

The Network ISSO at (Company or User Agency Name) and the IS Security Officer at (Name of other site) will indoctrinate system operators and support personnel concerning:

a. The need for sound security practices for protecting information handled by their respective IS, including all input, storage, and output products.

b. The specific security requirements associated with their respective IS as they relate to Protection Level 1 and operator access requirements.

c. The security reporting requirements and procedures in the event of a system malfunction or other security incident occurs.

d. What constitutes an unauthorized action as it relates to system usage.

e. Their responsibility to report any known or suspected security violations.

It is the responsibility of each individual operator to understand and comply with all required procedures for using the (Name of Classified System at Company Site), as described in the SSP which is approved by the Defense Security Service (DSS).

The system user shall report all instances of any security violations to the ISSM (or Network ISSO if located at company) at (Company Name). In addition, the User Agency IS Security Officer (or Network ISSO if located at User Agency) will report any security violations to the system.

4. Interconnect Procedures

The 9.6 kbps communication link at (Host Site Name) will be available 24 hours per day. The operating system at the host IS automatically records all operators logging in and out. Receipt and dispatch records for dial-up connections must be maintained. (Note to Template User: Please see DSS ISL 02L-1, Question 11, for options on what records are required. This is available at www.dss.mil/seclib/index.htm.) When logged in, the operators at (Contractor or User Agency Name) will be able to access the system for the transfer of classified data.

All signers agree there are no further connections on this network to DISN networks, including the SIPRNet.

When the communications link between (User Agency) and (Company Name) is no longer required, communications between the two hosts will be disabled by removing the remote users from the "system password file" and physically disabling the encrypted link from the router, if applicable. Additionally, the user agency will notify DSS in writing of cancellation of the MOU.

5. Approval

The secure communication link between (User Agency) and (Company Name) shall not be initialized until approval of these procedures by DSS is indicated below.

Defense Security Service	(User Agency)
_____	_____
(Name of DAA)	(Name of User Agency Official and Rank)
Title	Title
Designated Approval Authority	Designated Approval Authority

Optional Signatures:

(Company Name)

_____

(Name of Management Official)
Title

(Name of Company)

_____

Name of Facility Security Officer
Facility Security Officer

(Name of User Agency)

_____

Name of Security Official
Title